netVigilance

ScoutNews Team **May 6, 2005**
Issue # 17

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Lost laptops prove to be big security hole, what to do if you are hacked and of course, Phishing is good.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Secrets recovered from disposed laptop purchased for £80**

A lesson to us all; destroy hard drive data before throwing away those old computers. The Penetration testing firm, SecureTest; Oxon, UK found some sensitive Ministry of Defense information on a IBM ThinkPad that they recovered from a trash collector. Ken Munro of SecureTest said that it appeared to be a MoD supplier's discarded laptop.

This could be a very easy was for a hacker to access to sensitive and damaging data, if it were them doing the dumpster-diving instead of the whitehats at SecureTest.
The Register

Full Story:
http://www.theregister.co.uk/2005/04/26/tip_secret_laptop/

❖ Genetics Professor tries to scare laptop thief into returning extremely valuable data.

A genetics professor from University of California at Berkeley attempted to frighten the thief of his laptop into quietly returning the machine. The professor announced to students that some very sophisticated (albeit nonexistent) tracking measures would soon find the thief, then went on to disclose that his laptop also contained some very sensitive data. His attempts to intimidate the thief to return the laptop, only brought him ridicule and lampoon.

The likelihood of the thief ever returning the laptop is extremely low. Now that he knows that he is in possession of a lot more than test answers; he certainly won't turn himself in.

CMP

Related Links:
http://blastradius.blogspot.com/2005/04/world-of-pain.html - (contains profanity)
http://www.securitypipeline.com/news/161600257

❖ US-CERT documents Trojan, Virus recovery steps

The Dept. of Homeland Security; Computer Emergency Response Team (US-CERT), has a document outlining the steps to safely and securely recover from a Trojan or Virus attack to your system.

The documents can be found on the US-CERT website below. The process defined by Michael D. Durkota of US-CERT, gives specific guidelines for completing the following 7 steps necessary to fully recover from a cyber attack:

1. Call IT support
2. Disconnect from the internet
3. Backup important files
4. Install Anti-Virus and Scan for vulnerabilities

5. Re-install OS
6. Restore your files
7. implement safeguards and policies to prevent an infection.

US-CERT

Related Links:
http://www.us-cert.gov/reading_room/trojan-recovery.pdf

- **Phishing Report: Popularity of the sport is growing astronomically**

Network World reports that Phishing is one of the fastest growing forms of hacker attack. Even though businesses, vendors and users are getting more aware of the threat and more savvy in avoiding it; the Phishers are getting more sophisticated.

Phishers are not so blatantly asking for personal information upfront but using the technique to gain access to computers and scour personal information from there in what's know as a blended attack.

Full Story:

New Vulnerabilities Tested in SecureScout

- **13224 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB14)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13225 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB15)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13226 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB16)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13227 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB17)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13228 Oracle Database Server - Oracle HTTP Server component unspecified error (apr-2005/DB18)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13229 Oracle Database Server - Oracle HTTP Server (SSL) component unspecified error (apr-2005/DB19)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13230 Oracle Database Server - Oracle HTTP Server (SSL) component unspecified error (apr-2005/DB20)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **13231 Oracle Database Server - Oracle HTTP Server (SSL) component unspecified error (apr-2005/DB21)**

An unspecified error in the Oracle HTTP Server component can potentially be exploited to disclose or manipulate information.

Test Case Impact: **Gather Info** Vulnerability Impact: **High** Risk: **Attack**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt
http://secunia.com/advisories/14935/

Product Homepage:
http://www.oracle.com/

CVE Reference: None.

- **15619 ArGoSoft 1.8.x Mail Server Cross-Site Scripting Vulnerability (SMTP Check)**

ShineShadow has discovered a vulnerability in Argosoft Mail Server, which can be exploited by malicious people to conduct cross-site scripting.

Certain input passed in mails is not properly sanitised before being used. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious mail is viewed.

Example:
The "src" parameter in the "IMG" tag.

The vulnerabilities have been confirmed in version 1.8.7.6. Other versions may also be affected.

Test Case Impact: **Gather Info** Vulnerability Impact: **Medium** Risk: **Attack**

References:

http://www.argosoft.com/mailserver/default.aspx
http://secunia.com/advisories/15100/

CVE Reference: None.

- **15620 ArGoSoft 1.8.x Mail Server Script Insertion Vulnerability (SMTP Check)**

ShineShadow has discovered a vulnerability in Argosoft Mail Server, which can be exploited by malicious people to conduct script insertion attack.

Input passed to certain parameters in the user settings isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

The vulnerabilities have been confirmed in version 1.8.7.6. Other versions may also be affected.

Test Case Impact: **Gather Info** Vulnerability Impact: **Medium** Risk: **Attack**

References:

http://www.argosoft.com/mailserver/default.aspx
http://secunia.com/advisories/15100/

CVE Reference: None.

New Vulnerabilities found this Week

- **Oracle Web Cache / Application Server Two Vulnerabilities**

“cross-site scripting attacks, manipulate data, and bypass certain security restrictions”

Alexander Kornbrust has reported two vulnerabilities in Oracle9iAS Web Cache and Oracle Application Server, which can be exploited by malicious people to conduct cross-site scripting attacks, manipulate data, and bypass certain security restrictions.

1) Input passed to the "cache_dump_file" and "PartialPageErrorPage" parameters in "webcacheadmin" on port 4000 is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. This can further be exploited to write garbage to arbitrary files via the "cache_dump_file" parameter.

2) Restricted URLs on the Oracle Application Server (port 7779) can be accessed via the Web Cache on port 7778.

The vulnerabilities have been reported on a system with Oracle Application Server and Oracle9iAS Web Cache.

References:
http://www.red-database-security.com/advisory/oracle_webcache_CSS_vulnerabilities.html
http://www.red-database-security.com/advisory/oracle_webcache_append_file_vulnerabilitiy.html
http://www.red-database-security.com/advisory/oracle_webcache_bypass.html

- **Ethereal RSVP Protocol Decoding Denial of Service Vulnerability**

“Denial of Service”

Vade79 has reported a vulnerability in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the decoding of the RSVP protocol and can be exploited via a specially crafted RSVP packet.

Successful exploitation causes Ethereal to enter an infinite loop and stop responding.

The vulnerability has been reported in version 0.10.10. Prior versions may also be affected.

References:

http://secunia.com/advisories/15144/

- **Debian CVS Password Protection Bypass and Denial of Service**

“Denial of Service”

Debian has issued an update for cvs. This fixes two vulnerabilities, which can be exploited by malicious people to bypass password protection or cause a DoS (Denial of Service).

1) A security issue makes it possible to bypass the password protection and gain access to a repository when using the pserver access method.

2) A vulnerability can be exploited to crash the CVS server when the cvs-repouids file exists but doesn't contain a mapping for the current repository.

References:
http://www.debian.org/security/2005/dsa-715

- **HP-UX Unspecified TCP/IP Denial of Service Vulnerability**

“Denial of Service”

A vulnerability has been reported in HP-UX, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the PMTU discovery processing when receiving a specially crafted packet on any open connection.

Successful exploitation causes a DoS and requires a reboot of the system to regain functionality.

The vulnerability affects HP-UX B.11.00, B.11.04, B.11.11, B.11.22, and B.11.23 running TCP/IP (IPv4).

References:
http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01137

- **Argosoft Mail Server Cross-Site Scripting and Script Insertion**

“cross-site scripting and script insertion”

ShineShadow has discovered two vulnerabilities in Argosoft Mail Server, which can be exploited by malicious people to conduct cross-site scripting and script insertion attacks.

1) Certain input passed in mails is not properly sanitized before being used. This can be exploited to inject arbitrary HTML and script code, which

will be executed in a user's browser session in context of an affected site when the malicious mail is viewed.

Example:
The "src" parameter in the "IMG" tag.

2) Input passed to certain parameters in the user settings isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

The vulnerabilities have been confirmed in version 1.8.7.6. Other versions may also be affected.

References:
http://secunia.com/advisories/15100/

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the ‘security portal for information system security professionals’ is well founded.
http://www.infosyssec.org/infosyssec/

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net